Claims 1-31 are pending in the application. Claims 7-11 are allowed. Claims 1-5, 12-13, 19, 22-23, and 29 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,178,508 to Kaufman. Claims 14, 16-18, 20, 21, 24, 26-28, 30 and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,178,508 to Kaufman in view of the Examiner taking official notice.

Reconsideration is requested. The rejections are traversed. No new matter is added. Claims 1-31 remain in the case for consideration.

CLAIM REJECTIONS - 35 U.S.C. § 102

Claim 1 is directed toward an application server embodied in a computer, comprising: a user list, including a user name and a cleartext password associated with the user name; an authenticator to authenticate the cleartext password using an authentication server; a hasher to hash the cleartext password to produce a hashed password; a comparator to compare the hashed password with a received hashed password; and a client services provider to receive the received hashed password from a workstation and to transmit a result from the comparator to the workstation.

Claim 12 is directed toward a method for authenticating a user on an application server, comprising: receiving a user name and a hashed password from a first workstation; determining a cleartext password associated with the user name; authenticating the cleartext password to a second password using an authentication server; determining a hashing algorithm used by the first workstation; hashing the cleartext password using the hashing algorithm to produce a computed hashed password; comparing the received hashed password with the computed hashed password; and if the received hashed password matches the computed hashed password, authenticating the user.

Claim 22 is directed toward an article comprising a machine-accessible medium having associated data, wherein the data, when accessed, results in a machine performing: receiving a user name and a hashed password from a first workstation; determining a cleartext password associated with the user name; authenticating the cleartext password to a second password using an authentication server; determining a hashing algorithm used by the first workstation; hashing the cleartext password using the hashing algorithm to produce a computed hashed password;

comparing the received hashed password with the computed hashed password; and if the received hashed password matches the computed hashed password, authenticating the user.

In contrast, Kaufman teaches a system for access to encrypted data files by a plurality of users. A number of users each provide their passwords to the system (*see* Kaufman, column 7, lines 6-10, 26-43). The system hashes the individual passwords, concatenated with a salt value, to determine hashed passwords (*see* Kaufman, column 7, 6-9). These hashed passwords are compared with hashed password stored in a table in the data file (*see* Kaufman, column 7, lines 10-25). Once a quorum of users has provided recognized hashed passwords, the hashed passwords are combined and rehashed, then used to recover a file key that is used to encrypt data in the data file (*see* Kaufman, column 7, lines 44-56).

First of all, Kaufman is directed to a totally different invention than the claims. Kaufman is concerned with enabling access to an encrypted file where a number of people, but not necessarily all users, must each provide their own passwords to permit access to the encrypted file. According to Kaufman, "[o]ne mechanism . . . is to allow access to the secured information by subset, or quorum, of the total group if users" (*see* Kaufman, column 1, lines 51-53). Kaufman continues to say that the objective is "a security system which is useful for cryptographic systems, but can easily be maintained and can recover if passwords are forgotten" (*see* Kaufman, column 2, lines 20-22). In contrast, the claimed invention does not require multiple users be authenticated before any one of them is granted access to the resource.

Second, Kaufman does not teach storing cleartext passwords. According to Kaufman, "[t]he cryptographically hashed passwords are *never* kept in an unprotected, or unhashed, state in memory . . ." (*see* Kaufman, column 2, lines 38-39; emphasis added). Kaufman reinforces this point more than once: "[a]nyone gaining access to the unencrypted header file cannot obtain the passwords themselves" (*see* Kaufman, column 2, lines 47-48); "actual passwords do not appear in either the cleartext header of the file or in the encrypted portion of the file" (*see* Kaufman, column 8, lines 35-37).

Kaufman makes this point indirectly as well. In FIG. 2, where Kaufman shows the structure of the data file, Kaufman shows two tables stored in the unencrypted portion of the data file include two columns. In table 208, each user name is associated with a hashed version of the user's password (concatenated with the salt value) (*see* Kaufman, column 4, lines 19-24). In table 214, different combinations of users, who can constitute a quorum, are associated with a

particular encryption of the file key, so that when a particular quorum of users inputs their passwords, the input passwords, suitably hashed, can be used to recover the file key, which can then be used to access the encrypted data (*see* Kaufman, column 5, lines 7-43). In neither table is any cleartext password stored.

As claims 1, 12, and 22 all recite a cleartext password, the Examiner's assertion, without detail, that "Kaufman discloses the limitations of these claims (see at least the abstract and fig. 5)" (*see* Office Action dated May 9, 2007, page 2) is incorrect: Kaufman specifically teaches away from the claimed invention.

Further, claims 1, 12, and 22 all recite an authentication server used to authenticate the cleartext password. Nowhere does Kaufman mention any type of server, let alone an authentication server. To the contrary, Kaufman relies on the hashed passwords stored in the unencrypted portion of the file to authenticate the user. Kaufman does not use an authentication server for any purpose, and so does not disclose an authentication server.

As Kaufman does not teach or suggest storing a cleartext password or an authentication server, claims 1, 12, and 22 are patentable under 35 U.S.C. § 102(b) over Kaufman. Accordingly, claims 1, 12, and 22 are allowable, as are dependent claims 2-6, 13-21, and 23-31.

Claim 3 is directed toward an application server according to claim 2, wherein hasher includes a second hashing algorithm associated with the workstation.

The Examiner indicates that Kaufman teaches the features of claim 3 at column 5, lines 53-66. In the cited portion, Kaufman discusses the use of the concatenator as input to a one-way hash function. The Applicant recognizes that Kaufman does state that "[i]t is important that the hashing technique used in the second operation is different than the hashing technique used in forming table 208. . ." (*see* Kaufman, column 5, lines 43-46). But the Examiner is misapplying Kaufman. Kaufman shows two hash functions in FIG. 2: HASH1 (used in table 208) and HASH2 (used in table 214). In column 5, lines 43-46, Kaufman is emphasizing that the two hash functions used in tables 208 and 214 should be different. But all hashed passwords in a given table of Kaufman are hashed using the same hash function. Put another way, the same hash function is used for all users in a specific portion of the Kaufman system. The analogous situation in the claimed invention could occur only if all users' passwords were hashed for authentication using the same hash function: this is specifically contrary to claim 3, where

passwords reeeived from different workstations are hashed using different hashing algorithms for authentication purposes. Thus, Kaufman does not teach that the passwords used by different users could be hashed using different hashing algorithms, as described in claim 3.

Because Kaufman does not teach or suggest using different hash functions to has different passwords from different users, claim 3 is patentable under 35 U.S.C. § 102(b) over Kaufman. Accordingly, claim 3 is allowable.

Claim 19 is directed toward a method according to claim 12, wherein determining a cleartext password includes: determining that the cleartext password does not exist on the application server; requesting from the user the cleartext password; and receiving from the user the cleartext password.

Claim 29 is directed toward an article according to claim 22, wherein determining a cleartext password includes: determining that the cleartext password does not exist on the application server; requesting from the user the cleartext password; and receiving from the user the cleartext password.

The Examiner rejects claims 19 and 29 on the same basis as claims 1, 12, and 22. But as noted above, Kaufman does not teach or suggest an authentication server. Without an authentication server, Kaufman cannot anticipate claims 19 and 29 under 35 U.S.C. § 102(b). Accordingly, claims 19 and 29 are allowable.

CLAIM REJECTIONS - 35 U.S.C. § 103

Claim 16 is directed toward a method according to claim 12, wherein determining a hashing algorithm used includes selecting the hashing algorithm from a plurality of hashing algorithms.

Claim 17 is directed toward a method according to claim 16, further comprising adding a new hashing algorithm to the plurality of hashing algorithms.

Claim 18 is directed toward a method according to claim 17, wherein adding a new hashing algorithm includes associating the hashing algorithm with at least one of a set of workstations, the set of workstations including the first workstation.

Claim 26 is directed toward an article according to claim 22, wherein determining a hashing algorithm used includes selecting the hashing algorithm from a plurality of hashing algorithms.

Claim 27 is directed toward an article according to claim 26, the machine-accessible data further including associated data that, when accessed, results in adding a new hashing algorithm to the plurality of hashing algorithms.
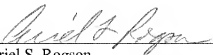
Claim 28 is directed toward an article according to claim 27, wherein adding a new hashing algorithm includes associating the hashing algorithm with at least one of a set of workstations, the set of workstations including the first workstation.

The Examiner acknowledges that Kaufman does not teach or suggest the features of these claims (*see* Office Action dated May 9, 2007, page 3). The Examiner takes official notice that "these elements are well known in the art of security systems". The Applicant traverses the Examiner's official notice. The Applicant does not believe it is "well known in the art of security systems" to use multiple different hashing algorithms in hashing passwords for users in the same "security system". And without using different hashing algorithms, there would be no impetus to select a hashing algorithm, as recited in claims 16-18 and 26-28. Under M.P.E.P. § 2144.03, the Examiner should provide documentary evidence to support the assertion that the features of these claims are well known in the art, or the Examiner should withdraw the rejection.

For the foregoing reasons, reconsideration and allowance of claims 1-31 of the application as amended is requested. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
210 SW Morrison Street, Suite 400
Portland, OR 97204
503-222-3613
Customer No. 45842